COGNITUM Software

go:Identity

Garantir la confiance des identités numériques

Une Gestion des Identités préconfigurée - Puissante, Simple, et Sécurisée

Le Problème

Une gestion fine des autorisations est essentielle pour la mise en place d'une infrastructure informatique sécurisée.

Sans une synchronisation intégrée des données de l'organisation et de ses employés à partir du système RH, et sans définition précise des processus pour gérer les habilitations, on observe de nombreuses failles dans la sécurité et des infractions aux règles internes qui ont pu être définies.

Cependant, les budgets informatiques souvent limités empêchent souvent de mettre en œuvre les mesures indispensables pour la gestion des identités et des accès.

Le Souhait

Facilité de travail et sécurité maximale en un temps réduit

- Réduisez les efforts d'administration d'AD Azure, LDAP, SA, SharePoint, ERP, CRM, etc.
- Réalisez régulièrement des opérations de recertification des utilisateurs et des rôles (pour les auditeurs)
- Migrez vos applications vers le cloud (Exchange / Lotus Notes vers Office 365, SharePoint, etc.)
- Administrez facilement les autorisations de partage de fichiers et les accès VPN
- Accédez aux demandes d'accès informatique par une interface Web en libre-service, contrôlées par des workflows d'approbation
- Libérez l'administration informatique de tâches répétitives sujettes aux erreurs
- Accédez à toutes les applications avec une seule authentification (SSO + Fédération)
- Recevez des rapports détaillés sur «Qui a eu / autorisé / retiré l'autorisation, quand, depuis quand, jusqu'à quand»
- Améliorez la sécurité informatique

La Solution

Une solution de gestion des identités rapidement déployable

go:Identity est un logiciel de gestion d'identités complète, centralisé et prêt à l'emploi pour toute taille d'organisation.

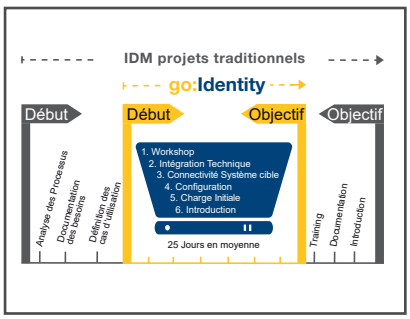
go:Identity gérera les identités, les rôles et les comptes d'utilisateurs, ainsi que les autorisations, dans n'importe quel système cible.

go:Identity est mis en oeuvre en 25 jours de projet en moyenne pour tout type de projet. Diverses fonctionnalités telles que l'affectation et la suppression des habilitations utilisateurs, le libre-service des utilisateurs et les workflows d'approbation sont déjà intégrés.

Les Principaux Avantages

Simple, sûre et efficace

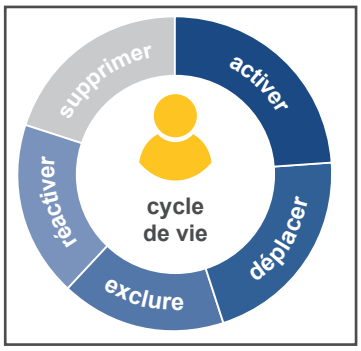
- Automatisation de nombreuses taches manuelles
- Amélioration de la sécurité
- Contrôle des accès et des autorisations
- Restitution fiable des données sous forme de rapports
- Préservation de l'intégrité des données
- Réduction du taux d'erreurs
- Normalisation qualitative des données
- Déploiement rapide



... avec un faible risque

L'approche "prête à l'emploi" réduit considérablement les risque du projet. Grâce à l'intégration des meilleures pratiques, les fonctions développées renforcent leur pertinence et leur adéquation aux besoins de l'entreprise étendue.

Caractéristiques



Gestion du cycle de vie des utilisateurs

go:Identity assure une gestion complète du cycle de vie des employés. Toute évolution des personnes (embauche, départ, changement de position, etc…) entraîne une modification automatiquement gérée par un processus workflow qui peut être suivi afin d'en assurer la conformité.

Fonctionnalités automatisées et manuelles :

- Création et modification d'identités – automatiquement depuis des données RH ou manuellement via l'interface utilisateur
- Désactivation ou suppression des identités ainsi que des permissions associées – automatiquement à une date fixe

Import des données RH automatisé

Les données RH doivent être complètes, à jour et cohérentes dans tous les systèmes.

go:Identity propose une interface qui permet d'importer des données RH afin de mettre à jour automatiquement les données de façon régulière :

- Création de nouvelles identités
- Génération d'identifiants utilisateur et adresse email unique
- Mise à jour d'identités existantes
- Désactivation ou suppression des employés ayant quitté l'organisation, absents des données RH ou inactifs

Administration des Autres Identités

Les identités externes (sous-traitants, employés temporaires…) n'ont généralement pas de compte personnel et ne sont pas importées depuis des données RH dans le système.

go:Identity offre la possibilité de gérer manuellement les identités externes en garantissant la sécurité et le respect des conformités :

- Sécurisation des identités externes grâce à un processus d'approbation pour leur création/modification
- Révocation automatique des autorisations obsolètes, par déclencheur spécifique ou à une date fixe

Self-Service Utilisateur

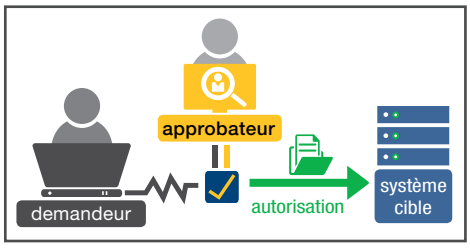
Si la gestion des identités externes (clients, partenaires, prospects, étudiants, etc…) est nécessaire, **go:Identity** propose une interface de libre-service en option. Les cas d'utilisation CIAM (Consumer Identity and Access Management) sont pris en charge pour les organisations qui ont besoin de gérer des identités de clients. Cette interface peut être combinée avec une solution Web SSO pour un contrôle d'accès complet vers toutes les applications Web afin de garantir un meilleur service en ligne de l'organisation.

Provisioning des Comptes Utilisateurs et Autorisations

Le provisioning des habilitations aux systèmes cibles prends beaucoup de temps, parfois même plusieurs jours, et il est souvent difficile de déterminer si un accès a été accordé.

go:Identity se connecte à une variété de systèmes tels que Active Directory, LDAP, Lotus Notes, SAP, des bases de données, mainframe, et bien d'autres, automatisant ainsi la gestion des comptes et des autorisations :

- Gestion centralisée des comptes systèmes, autorisations et mots de passe
- Blocage et suspension des droits d'accès



Affichage et analyse des autorisations sur les dossiers de partage de fichiers

go:Identity affiche toutes les autorisations de partage de fichiers d'une identité ou tous les droits d'accès à un dossier de partage de fichiers spécifique. À cette fin, les autorisations NTFS sont liées aux appartenances réelles aux groupes AD. De cette façon, même les autorisations attribuées involontairement deviennent visibles.

Toutes les informations peuvent être trouvées dans un lieu unique : la vue centrale d'autorisation de vos identités. Les exceptions sensibles peuvent être identifiées facilement, permettant un meilleur contrôle dans la gestion des accès sur les partages de fichiers.

Reporting und Auditing

go:Identity maintient les données nécessaires pour des rapports détaillés. Des modèles de rapports personnalisés peuvent être ajoutés.

Les données d'Audit permettent d'accéder rapidement aux informations critiques pour assurer la conformité et la gouvernance entre les identités. La fonctionnalité d'Audit de **go:Identity** permet de répondre aux questions suivantes :

- De quelles autorisations un employé dispose-t-il et quand les a-t-il reçus ou perdus ?
- Qui a approuvé quelles tâches et quand ?
- Quelles données ont été modifiées ?

Processus Workflow et Re-certifications

Les processus d'approbations sont configurés et mis à jour depuis le portail de workflow go:Identity. Celui-ci offre également la possibilité de gérer et de mettre à jour le flux de travail de toute la solution go:Identity. Les campagnes de re-certifications permettent aux responsables de gérer la re-certification des employés grâce à des processus d'attestations.

La confirmation périodique de l'accès des employés peut être lancée à partir du portail. Cette re-certification régulière garantit que seuls les utilisateurs identifiés et confirmés obtiennent ou perdent l'accès aux systèmes.

Vue d'ensemble des processus fonctionnels :

- Processus d'approbation des habilitations
- Traitement des identités externes
- Confirmation cyclique des identités, rôles et unités d'organisation sous des périodes de temps définis

Conformité Réglementaire

Les données d'identités sont de plus en plus strictement réglementées (par exemple GDPR, HIPAA et SOX, etc.), et il est important de respecter les directives à mesure qu'elles continuent d'évoluer. En outre, les organisations sont davantage sensibilisées sur l'exposition de leurs données et à la manière dont elles sont utilisées.

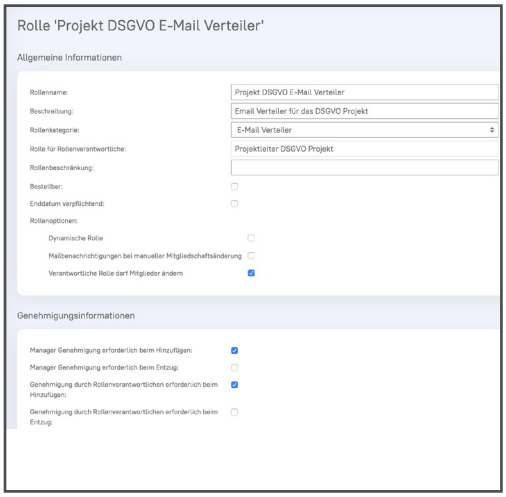
go:Identity prend en charge les exigences actuelles des directives et continuera à les maintenir et à les faire évoluer si nécessaire.

Interface d'Administration pour le Maintien des Rôles

Dans go:Identity, les rôles sont l'outil central de gestion et d'attribution des autorisations. En fonction de vos objectifs, votre administrateur peut définir différents rôles via l'interface d'administration.

Tout rôle peut soit déclencher une autorisation réelle sur un système cible, soit mener à un regroupement d'identités. L'interface d'administration vous permet de gérer les rôles et de contrôler les processus d'approbation et les notifications pour chaque rôle :

- Nom du rôle, catégorie et description
- Le rôle est-il disponible et est-t-il limité dans la durée ?
- Le manager doit-il approuver ?
- Un autre groupe ou responsable doit-il approuver ?
- Qui est le propriétaire du rôle ? Doit-il approuver ?
- Qui doit recevoir une notification du résultat à la fin du processus d'approbation ?



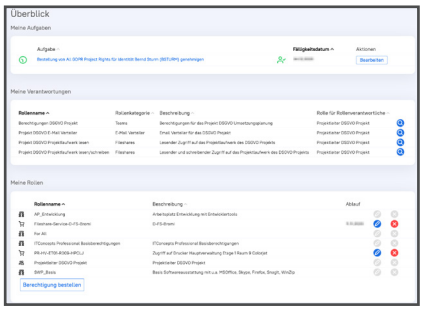
Les rôles peuvent être facilement attribués et gérés par les responsables ou les propriétaires des systèmes, allégeant ainsi la charge IT. Ces taches sont accomplies par les collaborateurs qui contrôlent ainsi l'accès aux données dont ils sont responsables.

Tableau de bord Central pour les Employés

Défini comme point initial et central de l'application, le tableau de bord présente à chaque utilisateur les habilitations qui lui sont attribuées, et permet aussi de formuler de nouvelles demandes d'habilitations, ou même de les restituer. Les processus d'approbation sont automatisés et chaque utilisateur peut suivre l'évolution et le statut de sa demande.

Fonctions additionnelles en self-service :

- Changement et réinitialisation des mots de passe
- Délégation
- Visualisation et modification de ses propres données



Unités d'Organisation et Management

go:Identity propose un module de gestion des structures hiérarchiques et de leurs responsables, ou managers. Ces unités organisationnelles permettent également l'attribution d'autorisations standard héritées de l'arborescence organisationnelle.

Détails Techniques

Interface Utilisateur

- Interface accessible depuis tout navigateur Web
- Multilingues (DE, EN, FR, + autres langages selon besoins)
- Interface graphique personnalisable (adaptable à toute charte graphique existante)

Connection aux systèmes cibles

- Connection vers des systèmes existants, par ex. Microsoft Active Directory, Azure AD, Exchange, SharePoint, SAP, LDAP
- Modules additionnels disponibles pour les connexions :
  - Notes
  - Bases de données, par exemple Oracle, MSSQL, MySQL und PostgreSQL
  - Linux et Unix
- Des systèmes spécifiques peuvent être intégrés via la structure flexible des connecteurs

Spécifications

- La solution est fournie en tant que machine virtuelle (VM)
- Système préconfiguré – pas d'installation fastidieuse
- Workflows et processus d'approbations prêts à l'emploi – des ajustements restent cependant possibles
- Intégration, mise en service et opération sur site ou hébergée
- Aucun engagement par abonnement – résiliation annuelle possible

go:Identity

La gestion standardisée des utilisateurs « prête à l'emploi »

- ✓ **go:fast** – Productivité Améliorée
- ✓ **go:cost-effective** – Solution rentable
- ✓ **go:secure** – Audit-friendly et Transparent
- ✓ **go:easy** – Contrôle de l'Attribution des Autorisations

COGNITUM Software

go:Identity

COGNITUM Software combine plusieurs décennies d'expérience dans le développement de ses propres produits pour la gouvernance des identités et des accès.

Dans les environnements informatiques hétérogènes d'aujourd'hui, la gouvernance des identités et des accès est un élément central d'une infrastructure informatique sécurisée. Grâce à notre expérience pratique complète dans le conseil, la mise en œuvre et notre expertise en matière de solutions de gouvernance d'identité et d'accès, nous avons développé un logiciel qui est déployable rapidement et rentable - pour toute entreprise, quelle que soit son secteur d'activité et sa taille.

COGNITUM Software est issu du groupe ITConcepts, un leader mondial des services informatiques et intégrateur de systèmes agnostiques.

COGNITUM Software Team GmbH
Leitschweg 2c, 38448 Wolfsburg, Allemagne • Téléphone: +49 5361 8349527 • Email: info@cognitum-software.com • Web: www.cognitum-software.com